PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-229861
(43)Date of publication of application : 16.08.2002

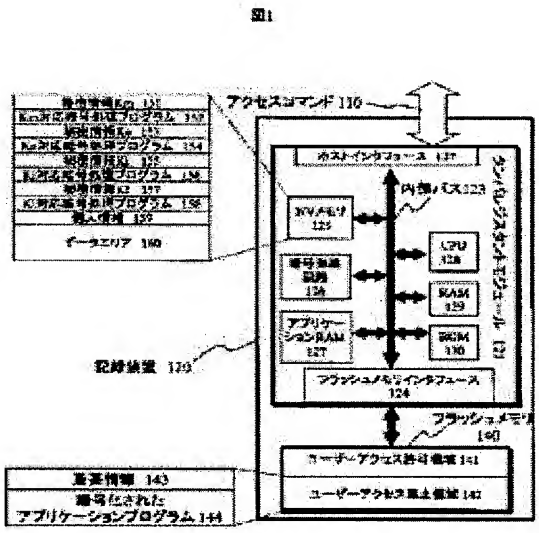
(51)Int.Cl. G06F 12/14
G06F 3/06
G06F 3/08
G06F 1/00
G06K 19/073
G11C 16/02
H04L 9/08
H04L 9/10

(21)Application number : 2001-030384
(22)Date of filing : 07.02.2001

(71)Applicant : HITACHI LTD
(72)Inventor : IGUCHI SHINYA
TSUNEHIRO TAKASHI
TSUNODA MOTOYASU
ISHIHARA HARUJI
MIZUSHIMA EIGA
TOTSUKA TAKASHI

(54) RECORDING DEVICE WITH COPYRIGHT PROTECTING FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an inexpensive recording device capable of recording a lot of data having a high secrecy by mounting two kinds of semiconductor nonvolatile memories of different properties on the recording device using a semiconductor memory, and selecting written data with the recording device.
SOLUTION: A tamper resistant module 121 and a flash memory 140 are mounted on the recording device 120. A CPU 128 in the tamper resistant module 121 judges the secrecy of data sent by an access command 110. A small amount of data having high secrecy is recorded in an NV memory 125, a large amount of data having high secrecy is ciphered and recorded in the flash memory 130, and data having low secrecy is directly recorded in the flash memory 140.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（A）**　(11)特許出願公開番号
特開2002－229861
（P2002－229861A）
(43)公開日　平成14年８月16日(2002.8.16)

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
G06F 12/14	320	G06F 12/14	320F 5B017
			320B 5B025
3/06	304	3/06	304H 5B035
3/08		3/08	C 5B065
1/00		9/06	660D 5B076

審査請求　未請求　請求項の数７　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願2001－30384(P2001－30384)

(22)出願日　平成13年２月７日(2001.2.7)

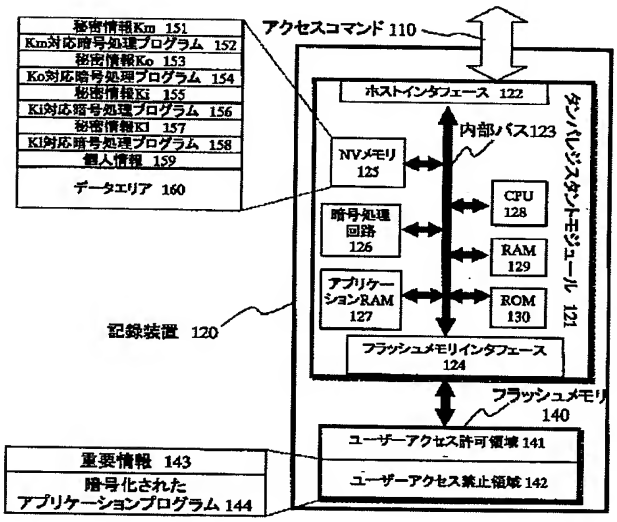
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　井口　慎也
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　常広　隆司
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　著作権保護機能つき記録装置

(57)【要約】
【課題】本発明は、半導体メモリを用いた記録装置に、特性の違う二種類の半導体不揮発性メモリを搭載し、それらに書きこむデータを記録装置で選別することで、秘匿性の高いデータを多量に記録することが可能な、記録装置を安価に実現する。
【解決手段】記録装置１２０にタンパレジスタントモジュール１２１とフラッシュメモリ１４０を搭載し、アクセスコマンド１１０によって送信されてきたデータの秘匿性をタンパレジスタントモジュール１２１内のＣＰＵ１２８が判断し、秘匿性の高い小容量のデータをNVメモリ１２５へ、秘匿性の高い大容量のデータは暗号化してフラッシュメモリ１４０へ、そして秘匿性の低いデータをそのままフラッシュメモリ１４０へ記録する手段を有する記録装置。

図1



【特許請求の範囲】
【請求項１】内部不揮発性メモリを有するメモリコントローラ及び外部不揮発性メモリとを具備し、
前記メモリコントローラは、外部装置と接続されるホストインターフェイス、上記外部不揮発性メモリと接続されるメモリインターフェイス、前記ホストインターフェイスとメモリインターフェイスと接続された内部バス、前記内部バスに接続されたＣＰＵ、内部不揮発性メモリ及びアプリケーション格納用メモリとを有し、
前記内部不揮発性メモリは、ユーザー個人情報であるKi、ユーザー端末装置情報であるKo、暗号化処理プログラムを外部不揮発性メモリからメモリコントローラのアプリケーション格納用メモリに復号化して格納するための情報であるKm及びアプリケーションダウンロード時の情報であるKLのいずれかの秘密情報と、前記秘密情報に対応する暗号化処理プログラムとを格納することが可能であり、
前記外部不揮発性メモリは、ユーザーアクセス許可領域とユーザーアクセス禁止領域とを有し、
コンテンツデータを前記ユーザーアクセス許可領域に格納し、
前記メモリコントローラが使用するファームウェアを前記ユーザーアクセス禁止領域に格納することが可能であることを特徴とするパッケージされた記録装置。
【請求項２】暗号化されたアプリケーションプログラムを前記ユーザーアクセス禁止領域に格納することが可能であることを特徴とする請求項１記載のパッケージされた記録装置。
【請求項３】コマンドもしくは書込データの属性を前記メモリコントローラの前記ＣＰＵが解析して、格納先を前記外部不揮発性メモリ又は前記内部不揮発性メモリとに振り分ける機能を有することを特徴とする請求項１又は２記載のパッケージされた記録装置。
【請求項４】前記内部不揮発性メモリが容量不足か否かを前記ＣＰＵが判定して、Ki、Ko、Km及びKLのいずれかに対応する前記暗号化処理プログラムのデータもしくはそれを暗号化したデータを外部不揮発性メモリに格納することが可能であることを特徴とする請求項３記載のパッケージされた記録装置。
【請求項５】前記外部不揮発性メモリは、多値のフラッシュメモリを使用して構成されていることを特徴とする請求項１、２、３又は４記載のパッケージされた記録装置。
【請求項６】請求項１記載のパッケージされた記憶装置を実装したユーザー端末装置とサービスプロバイダが有するサーバとのデータ転送方法であって、
前記ユーザー端末装置のIDであるKoを前記記録装置から前記ユーザー端末装置に送信し、
前記Koを前記ユーザー端末装置から前記サービスプロバイダのサーバへ両者が保有している共通の鍵で暗号化して送信し、
前記サービスプロバイダのサーバで前記Koを共通の鍵で復号化して取り出して前記Koを共有し、
前記Koを利用して前記ユーザー端末装置と前記サービスプロバイダのサーバ間でデータを暗号化して送受信することで、前記ユーザー端末装置と前記サービスプロバイダのサーバ間で、第３者がデータを取り出すことができない安全な外部送信経路を確立し、
さらに、前記記録装置でKiを前記サービスプロバイダのサーバが既知の鍵で暗号化して前記ユーザー端末装置に送信し、
前記ユーザ端末装置から前記外部送信経路を通して暗号化された前記Kiを前記サービスプロバイダのサーバに送信し、
前記サービスプロバイダのサーバで復号化して前記Kiを共有し、
前記Kiを暗号化の鍵生成情報として利用することで、前記記録装置と前記サービスプロバイダのサーバとの間で安全な通信経路を確立し、
前記安全な通信経路で、前記サービスプロバイダのサーバから前記記録装置へデータを転送することを特徴とする方法。
【請求項７】請求項１、２、３、４又は請求項５に記載の記録装置を搭載可能で、前記記録装置と秘密情報Kiを共有することで暗号化された通信を行い、前記記録装置からデータを読み出し復号化して再生する機能を有するデコーダ回路を有するユーザ端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、記憶装置及び記憶装置に接続される情報機器に関し、特に、情報機器と記録装置とのデータ転送の制御方式に関する。
【０００２】
【従来の技術】近年、インターネット等のネットワーク社会の発達によって、ネットワークに流通する音楽や画像といったコンテンツの著作権を保護するための技術の重要性が高まっている。著作権保護の技術として、暗号化・復号化に使用する秘密鍵を格納する秘密鍵記憶回路と、データを保存するデータ記憶回路を搭載し、書きこみ制御回路を用いて秘密鍵記憶回路に秘密鍵を書きこむ機能と、相手機器を認証する機能を有するメモリICカードが提案されている。この技術は、例えば、特開2000-163547号公報に開示されている。
【０００３】
【発明が解決しようとする課題】従来技術では、メモリICカード等のパッケージされた記憶装置上の記録媒体にすべてのデータが記録される。メモリICカード等のパッケージされた記憶装置は、コンテンツの盗難等を防止するため、カード外部から内部のデータを解析することが困難な構造(タンパレジスタントモジュール)を有する。

一般的に、タンパレジスタントモジュールを有するメモリICカード等のパッケージされた記憶装置は高価で、かつメモリの記憶容量が小さい。したがって、メモリICカード等のパッケージされた記憶装置に、秘匿性の高いデータを多量に格納することは非常に困難であった。

【０００４】また、従来技術では、メモリICカード等のパッケージされた記憶装置では、秘匿性の高いデータと低いデータが記録装置で判断することなしに、上位装置からの転送指示応じてそのままタンパレジスタントモジュールへ格納されていた。このため、秘匿しなくても良いデータまでタンパレジスタントモジュール内にすべて格納されることとなり、タンパレジスタントモジュール内の記憶領域を有効に活用できなかった。

【０００５】また、従来技術では、データ保存用の記憶領域としてEEPROM等の不揮発性メモリ（以下NVメモリ）が使用される。しかし、従来技術で使用されるNVメモリは書き換え可能な回数が少なく、多くのコンテンツを何度も入れ替えることが困難であった。

【０００６】さらに、従来技術では、上述したように、メモリICカード等のパッケージされた記憶装置の記憶容量が小容量なので、メモリICカード上でアプリケーションを実行する場合でも、プログラムの使用する記憶容量が小さいアプリケーションしか実行することが出来なかった。

【０００７】本発明の目的は、秘匿性の高いデータを安価にかつ多量に何度も保存できるパッケージされた記憶装置を提供することである。

【０００８】本発明の他の目的は、タンパレジスタントモジュール内の記録領域を有効利用することができる記憶装置を提供することにある。

【０００９】さらに、本発明の他の目的は、様々なアプリケーションが記録され、しかも規模の大きなアプリケーションが実行できるパッケージされた記憶装置を提供することにある。

【００１０】

【課題を解決するための手段】上記目的を達成するために、ＣＰＵ、RAM、ＲＯＭ、不揮発性メモリ及び暗号処理回路から構成されたタンパレジスタントモジュールと大容量なフラッシュメモリを用いて、タンパレジスタントモジュール内に記録装置固有の秘密鍵等を記録しておき、タンパレジスタントモジュール内の不揮発性メモリへ記録出来ない情報は、秘密鍵で暗号化したのちフラッシュメモリへ書き込む手段を備えた記録装置を構成する。

【００１１】上記他の目的を達成するために、タンパレジスタントモジュール内のＣＰＵが外部から送信されてきた情報の秘匿性を判断し、重要な情報はタンパレジスタントモジュール内部の不揮発性メモリへ記録し、通常の情報はフラッシュメモリへ記録するようにデータを振り分ける機能を搭載した記録装置を構成する。

【００１２】さらに、上記他の目的を達成するために、タンパレジスタントモジュール内でアプリケーションを実行するRAMを搭載し、アプリケーションをタンパレジスタントモジュール内の秘密鍵で暗号化し外部のフラッシュメモリの記録装置の利用者がアクセスできない領域に保存しておき、必要に応じて、フラッシュメモリからアプリケーションを読み出し、ＲＡＭへ展開して実行する機能を有する記録装置を構成する。

【００１３】

【発明の実施の形態】図１は、本発明が適用された記録装置１２０の構成図である。記録装置１２０は、タンパレジスタントモジュール１２１及びフラッシュメモリ１４０を有する。タンパレジスタントモジュール１２１は、外部から物理的な解析を行うことが困難なように構成された電子回路であり、ICカードなど、高度なセキュリティが要求される電子機器に使用される。内部バス１２３は、各回路間の情報を送受信するために使用される。フラッシュメモリインタフェース１２４は、フラッシュメモリ１４０とタンパレジスタントモジュール121とを接続するために使用される。

【００１４】ホストインタフェース１２２は、記録装置１２０と記憶装置１２０と接続される外部機器とのアクセスコマンド１１０の送受信に使用される。ＣＰＵ１２８は、記録装置１２０内の各回路を制御する。暗号処理回路１２６は、記録装置１２０内で暗号処理を行うためにＣＰＵ１２８によって使用される。RAM１２９は、データを一時的な記録するために使用されるワークRAMである。ROM１３０には、ＣＰＵ１２８が恒久的に利用するプログラム及びデータが記録される。NVメモリ１２５は、小容量で書き込み回数が少ない不揮発性メモリである。NVメモリ１２５は、外部から解析されると危険な情報が記録される。NVメモリ１２５としては、例えば、EEPROMなどがある。NVメモリ１２５には、以下の情報及びプログラムが格納される。

【００１５】秘密情報Km１５１には、タンパレジスタントモジュール１２１がフラッシュメモリ１４０へデータを読み書きする際に、データを暗号化、復号化するために使用する鍵の情報などが含まれる。Km対応暗号処理プログラム１５２は、秘密情報Km１５１を利用して暗号処理を行うアプリケーションである。

【００１６】秘密情報Ko１５３には、サービスプロバイダ１００のサーバ１８０と携帯端末１０３が、後述する公衆回線１０８に暗号化された通信経路を確立するために使用される証明書、鍵の情報などが含まれる。Ko対応暗号処理プログラム１５２は、秘密情報Ko１５３を利用して暗号処理を行うアプリケーションである。

【００１７】秘密情報Ki１５５には、サービスプロバイダ１００のサーバ１８０内の配信アプリケーション１８１と記録装置１２０が、後述する暗号化内部通信経路１０９を確立するために使用される記録装置証明書、鍵の

情報などが含まれる。Ki対応暗号処理プログラム１５６は、秘密情報Ki１５５を利用して暗号処理を行うアプリケーションである。

【００１８】秘密情報K1１５７には、ＣＰＵ１２８が実行するアプリケーションが暗号処理を行う際に必要な証明書、鍵の情報などが含まれる。K1対応暗号処理プログラム１５８は、秘密情報K１１５７を利用して暗号処理を行うアプリケーションである。尚、K1１５７は、アプリケーションによって独自の目的で使用される場合がある。K1１５７は、アプリケーションごとに複数存在する場合もある。

【００１９】NVメモリ１２５は、データエリア１６０を有する。データエリア１６０には、記録装置１２０を使用する者の個人的な情報、例えば、電話帳、スケジュール、クレジットカード情報、電子マネー、個人認証情報などが格納される。

【００２０】これらの重要個人情報(鍵情報等)は、フラッシュメモリ１４０に格納することも考えられるが、悪意のものがカードを破壊して、読み出す可能性があるので、外部からの読み出しが困難なタンパレジスタントモジュール１２１のNVメモリ１２５に格納する。

【００２１】アプリケーションRAM１２７は、ＣＰＵ128がアプリケーション実行時にフラッシュメモリ１４０から読み出した暗号化されたアプリケーション１４４の暗号を復号して実行するために使用される。

【００２２】フラッシュメモリ１４０は、一括消去書き込み可能な不揮発性メモリであり、例えば、記憶容量が大きい多値フラッシュメモリなどのフラッシュメモリチップが考えられる。フラッシュメモリ１４０は、ユーザアクセス禁止領域１４２及びユーザアクセス許可領域１４１を有する。ユーザアクセス禁止領域１４２に格納されたデータは、タンパレジスタントモジュール１２１内のＣＰＵ１２８のみによって消去及び書き込まれる。ユーザアクセス禁止領域１４２には、記録装置１２０が実行する暗号化されたアプリケーション１４４、記録装置１２０のファームウェア等の重要情報１４３等ユーザーによって操作されると困る情報が保存される。尚、ここのデータには、外部から改ざん不可能なように電子署名が付加される場合もある。ユーザーアクセス許可領域１４１は、記憶装置１２０に接続される外部装置から自由にアクセスすることが可能な領域であり、コンテンツ４０２、暗号化されたプログラム、その他特に外部に見られても問題のないデータが保存される。

【００２３】ＣＰＵ１２８が使用する多種多様なアプリケーションプログラムは、フラッシュメモリ１４０にあらかじめ暗号化されて格納される。暗号化されたアプリケーションプログラム１４４は、使用される前に、タンパレジスタントモジュール１２１に供給される。その際に、ＣＰＵ１２８は、Km１５１及びKm対応暗号処理プログラム１５２を用いて、アプリケーションプログラムを復号化して、アプリケーション RAM１２７にロードする。ロードが完了すると、アプリケーションプログラムは実行可能となる。一方、音声、画像等のコンテンツ４０２は、フラッシュメモリ１４０に格納される。この際、ＣＰＵ１２８は、アクセスコマンド１１０に応じてデータの格納先を自動的に解析する。解析手段の詳細は後述する。

【００２４】図2は、本発明が適用された記憶装置１２０の実施形態を使用したシステムの構成図である。携帯端末103は、記録装置１２０と接続され、記録装置１２０を利用してサービスプロバイダ１００と通信を行う機能を有する。携帯端末１０３は、表示画面１０４、スピーカ１０５、マイク１０６及びCCDカメラ１０７を有する。

【００２５】サービスプロバイダ１００は、記録装置１２０に対して、コンテンツ配信などを行うサーバ１８０を有する。サーバ１８０は、配信アプリケーション１８１、配信するコンテンツ１８２を有する。

【００２６】サービスプロバイダ１００と携帯端末１０３の間では、データの漏洩を防ぐために、公衆回線１０８上に、暗号化された通信経路を確立することが可能である。さらに、携帯端末１０３に接続された記録装置１２０は、サービスプロバイダ１００との間に確立された暗号化された通信経路内で、さらに暗号化された内部通信経路１０９を確立することも可能である。図では、内部通信経路１０９は携帯端末１０３にのみ示されているが、実際は、公衆回線１０８上にも経路が確保されている。詳細は後述する。

【００２７】サービスプロバイダ１００、携帯端末１０３及び記録装置１２０を用いた本システムでは、サービスプロバイダ１００と記録装置１２０がデータを送受信する際は、データは、サービスプロバイダ１００と携帯端末１０３との間、すなわち公衆回線１０８上で２重に暗号化され、携帯端末１０３と記録装置１２０との間では1重に暗号化される。携帯端末１０３等で利用される暗号処理方式によっては、サービスプロバイダ１００と携帯端末１０３間では、データはn+m重に暗号化され、携帯端末１０３と記録装置１２０間では、m重に暗号化される場合もある。尚、記録装置１２０を接続する機器は携帯端末１０３に限定されないし、公衆回線１０８は、有線回線でも無線回線でもよい。有線回線としては、光ケーブル等が考えられる。

【００２８】図3は、携帯端末１０３の構成図である。ＣＰＵ２０１は、携帯端末１０３の各回路を制御する。ＲＡＭ２０２には、ＣＰＵ２０１が利用するデータが一時的に保存される。ＲＯＭ２０３には、ＣＰＵ２０１が恒久的に利用する書き換えを行わないデータが記録される。携帯端末制御回路２０４は、携帯端末１０３と外部機器との情報の送受信などの処理を行う。入出力インタフェース２０５は、携帯端末１０３を利用する者のキー

入力、画面表示などの処理を行う。記録装置インタフェース２０７は、記録装置１２０との間で情報の送受信を行う。デコーダ回路２０６は、記録装置１２０から読み出した情報を、音声や映像などに復号する。バス２０８は、回路間における情報の送受信に使用される。

【００２９】図４は、デコーダ回路２０６の構成を示す図である。デコーダ回路２０６は、記録装置１２０から読み出したデータを復号してから再生するため、復号されたデータを外部からアクセスできないようにする必要がある。このため、デコーダ回路２０６は、タンパレジスタントモジュールになっている。制御回路３０１は、デコーダ回路２０６内の各回路を制御する。RAM３０２には、復号した情報などが一時的に記録される。ＲＯＭ３０３には、制御回路のプログラムなど恒久的に利用する情報で機密性が低いものが記録される。不揮発性メモリ３０６には、デコーダ回路２０６の証明書、記録装置１２０から取り出した暗号化されたデータを復号化するために必要な鍵など、機密性が高い情報が記録される。インタフェース３０７は、外部回路との接続に使用されるインタフェースである。バス３０８は、各回路間の情報の送受信に使用される。

【００３０】図５は、本発明が適用された記録装置１２０が用いられるシステムにおける通信方式の一例を示す図である。記録装置１２０と携帯端末１０３との間の情報の送受信は、アクセスコマンド１１０でおこなわれる。アクセスコマンド１１０は、階層化されたアクセスコマンド（以下、「階層化コマンド」と称する）４０５で定義される。物理アクセスコマンド４０８は、記録装置１２０とのデータの入出力など基本的なコマンドである。論理アクセスコマンド４０９は、物理アクセスコマンド４０８のデータとして送受信される。記録装置１２０及び携帯端末１０３は、物理アクセスコマンド４０８を解析し、データ領域から論理アクセスコマンド４０９を取り出して実行する。このようなコマンド構成にすることで、携帯端末１０３と記録装置１２０との間での基本的なコマンドに変更を加えることなく、容易にコマンドを拡張することが出来る。

【００３１】ライセンス４０１は、暗号化コンテンツ４０２を復号化するための鍵を含む情報である。暗号化コンテンツ４０２は、ライセンス４０１によって暗号化されたコンテンツである。ライセンス配信４０４の矢印は、サービスプロバイダ１００からネットワーク４０３、携帯端末１０３を介して記録装置１２０のタンパレジスタントモジュール１２１へライセンス４０１を配信する場合を示している。コンテンツ配信４０７の矢印は、サービスプロバイダ１００から記録装置１２０へコンテンツ４０２を配信する場合を示している。サービスプロバイダ１００と携帯端末１０３との間では、ライセンス４０１及びコンテンツ４０２は、階層化コマンド４０６を利用して配信される。携帯端末１０３と記録装置１２０との間では、ライセンス４０１は階層化コマンド４０５を利用して配信され、タンパレジスタントモジュール１２１へ格納される。コンテンツ４０２は、携帯端末１０３と記録装置１２０の間では、物理アクセスコマンド４０８のみを利用して記録装置１２０内のフラッシュメモリ１４０へ配信される。

【００３２】図１９は、物理アクセスコマンド４０８及び論理アクセスコマンド４０９の構成例を示す図である。物理アクセスコマンド４０８は、コマンドコード１８０１、長さ１８０２及びデータエリア１８０３から構成されている。コマンドコード１８０１は、コマンドタイプ１８１０、属性１８１１及びセキュリティレベル１８１２から構成されている。コマンドタイプ１８１０と属性１８１１には、図１９の表に示すような対応関係の情報が格納されている。属性１８１１とは、例えばデータが個人情報、鍵情報などであるか、他の一般的な情報であるか等を示すタグなどである。以下このような属性を表すデータを、属性データという。セキュリティレベル１８１２には、コマンドによって送信されるデータの機密性のレベルを示す情報が格納される。機密性のレベルは、本実施形態の場合、３段階に分かれている。セキュリティレベルは、送信されるデータの性質に応じて、アクセスコマンド１１０を発行する装置によって発行時にアクセスコマンド１１０に付加される。

【００３３】長さ１８０２には、データエリア１８０３の長さを表す情報が格納される。データエリア１８０３には、通常のデータの他に、論理アクセスコマンド４０９も含まれる。

【００３４】論理アクセスコマンド４０９は、コマンドコード１８０４、長さ１８０５及びデータ１８０６で構成される。コマンドコード１８０４は、物理アクセスコマンド４０８のコマンドコード１８０１と同一である。長さ１８０５には、データ１８０６に格納されるデータの長さを示す情報が格納される。データ１８０６には、実際のデータが格納される。

【００３５】階層化コマンド４０６とそれを構成する物理アクセスコマンド４１０と論理アクセスコマンド４１１も階層化コマンド４０５と同様な構成になっている。階層化コマンド４０６は、携帯端末１０３とサーバ１８０がネットワーク４０３を介して情報を送受信する場合に利用される。尚、階層化コマンド４０５と階層化コマンド４０６の具体的なコマンドコードなどは異なっていてもかまわない。

【００３６】図２０は、記録装置１２０が行うコマンド受信した階層化コマンドの振り分け処理を示すフロー図である。記録装置１２０は、物理アクセスコマンド４０８を受信する(１９０１)。記録装置１２０内のＣＰＵ１２８は、物理アクセスコマンド４０８のコマンドコード１８０１をチェックする(１９０２)。論理アクセスコマンド４０９が存在すれば、ＣＰＵ１２８は、論理アクセ

スコマンドの解析を実行する（１９０４）。ＣＰＵ１２８は、論理アクセスコマンド４０９を処理する（１９０５）。物理アクセスコマンド４０８に論理アクセスコマンド４０９が含まれていない場合は、ＣＰＵ１２８は、物理アクセスコマンド処理を実行する（１９０３）。コマンドの処理が終了すると、ＣＰＵ１２８は、データ選別処理を行い、秘匿性の高いデータと低いデータを識別してそれぞれのデータに適した領域に記録を行う(１９０６)。

【００３７】図２１は、ＣＰＵ１２８が実行するデータ選別処理１９０６を示したフロー図である。ＣＰＵ１２８は、携帯端末１０３より送信されてきた物理アクセスコマンド４０８又は論理アクセスコマンド４０９のコマンドタイプ１８１０がWRITEコマンドかどうか調べ（２００２）、WRITEコマンド以外なら処理を終了する（２００９）。コマンドタイプ１８１０がWRITEコマンドなら、ＣＰＵ１２８は、データエリア内のデータを調べ、属性１８１１に属性データが存在するか調べる（２００３）。属性１８１１に属性データが存在しないなら、ＣＰＵ１２８は、コマンドコードのセキュリティレベル１８１２をチェックする(２００４)。ＣＰＵ１２８は、セキュリティレベルが１なら、NVメモリ１２５の空き容量を調べ（２００５）、空き容量が十分あるなら、データをNVメモリ１２５へ格納する（２００６）。空き容量が十分ないなら、ＣＰＵ１２８は、データを暗号化して（２００７）、データをフラッシュメモリ１４０へ書き込む（２００８）。セキュリティレベルが２なら、ＣＰＵ１２８は、データを暗号化して（２００７）、データをフラッシュメモリ１４０へ書き込む（２００８）。セキュリティレベルが３なら、ＣＰＵ１２８は、データをフラッシュメモリ１４０へ書き込む（２００８）。ステップ２００３で属性１８１１に属性データが存在すると判断したら、ＣＰＵ１２８は、属性データの内容を判断する（２０１０）。属性データによって、アクセスコマンドによって送られてきたデータが小容量の機密データであると判断されるなら、ＣＰＵ１２８は、NVメモリ１２５の空き容量を調べ（２０１１）、空き容量があるなら、データをNVメモリ１２５へ格納する（２０１２）。空き容量が十分無いなら、ＣＰＵ１２８は、データを暗号化して（２０１３）、データをフラッシュメモリ１４０へ格納する（２０１４）。大容量の機密データと判断されると、ＣＰＵ１２８は、データを暗号化して（２０１３）、データをフラッシュメモリ１４０へ格納する（２０１４）。暗号化の必要がないなら、ＣＰＵ１２８は、データをそのままフラッシュメモリ１４０へ格納する（２０１４）。

【００３８】図６は、公衆回線１０８における暗号化された通信経路確立処理５１０及び暗号化内部通信経路確立処理５２０を示すフロー図である。これらの手順を一まとめにして暗号化通信経路確立処理５００と称する。

【００３９】公衆回線１０８における暗号化された通信経路確立処理５１０を説明する。携帯端末１０３は、秘密情報Ko１５３を記録装置１２０から取り出す（５０２）。携帯端末１０３は、秘密情報Ko１５３を暗号化してサービスプロバイダ１００へ送信する（５０３）。暗号化された秘密情報Ko１５３を受信したサービスプロバイダ１００のサーバ１８０は、秘密情報Ko１５３を復号化して取り出す（５０４）。その後の通信においては、サーバ１８０と携帯端末１０３が秘密情報Ko１５３で情報を暗号化して送受信する。これによって、暗号化された通信経路が確立される(５０６)。

【００４０】暗号化内部通信経路確立処理５２０を説明する。記録装置１２０は、秘密情報Ki１５５を暗号化し、携帯端末１０３及びサービスプロバイダ１００間で確立されている暗号化された通信経路を用いて、暗号化された秘密情報Ki１５５をサービスプロバイダ１００へ送信する（５０９）。暗号化された秘密情報Ki１５５を受信したサービスプロバイダ１００のサーバ１８０は、秘密情報Ki１５５を復号化して取り出す（５１０）。その後、サーバ１８０と記録装置１２０が秘密情報Ki１５５で情報を暗号化して情報を送受信する（５１１）。これによって、暗号化内部通信経路が確立される（５１２）。

【００４１】図７は、携帯端末１０３と記録装置１２０、サーバ１８０の間での著作権保護の基本的な流れを示す図である。この図では、サーバ１８０から記録装置１２０へ著作権を保護したいコンテンツ４０２を送信する場合について示している。各送信手順の表記は、図２２に示す表記法規定２１０１に従う。尚、図７においてはKs1はサーバ１８０が乱数などを使用して生成する。Ks2は記録装置１２０の暗号処理回路１２６が乱数などを使用して生成する。利用者が携帯端末１０３を操作して、コンテンツ取得を記録装置１２０へ指示すると、記録装置１２０がコンテンツ要求６０１を携帯端末１０３を通してコンテンツ４０２を保持しているサーバ１８０へ発行する。これによって記録装置１２０は、取得したいコンテンツ４０２に対応したＣｏｎｔｅｎｔ　ＩＤと記録装置１２０が正当な機器であることを証明する証明書C(Ka,KPmc¦¦Imc)をサーバ１８０へ送信する（６０２）。サーバ１８０が、コンテンツＩＤと証明書を受信すると、証明書をチェックする。証明書が正規のものであれば、記録装置１２０へセッション鍵E(KPmc,Ks1) を送信する（６０３）。セッション鍵Ks１を記録装置１２０が受信すると、セッション鍵Ｋｓ２を含めた様々な情報をE(Ks1,KPm1¦¦Ks2¦¦CRLUpdate) としてサーバ１８０へ送信する（６０４）。これを受信したサーバ１８０はライセンス４０１を含む様々な情報をE(Ks2,CRL¦¦ E(KPm1, TransacationID ¦¦ Acm ¦¦ Kc ¦¦ Acp))として記録装置１２０へ送信する（６０５）。続いて、サーバ１８０は、コンテンツ４０２を記録装置１２０へE(Kc,C

ontent)として送信する(６０６)。以下で説明する情報の送受信はここで述べた方式を利用する。

【００４２】図8は、記録装置１２０、携帯端末１０３及びサーバ１８０それぞれのソフトウェアの階層構造を表している。以下の記載では、サービスプロバイダ１００の記載を省略する。記録装置１２０では、暗号化計算部７０２の上にアプリケーション７０１が構成されている。アプリケーション７０１が、暗号化計算部７０２を利用して暗号処理などを行う。ソフトウェアはタンパレジスタントモジュール121に構成される。アプリケーション７０１は、記録装置１２０内のデータ処理から暗号化通信など記録装置が提供するサービスに応じたアプリケーション７０１が搭載される。暗号化計算部７０２は、暗号に関する計算処理を行う。暗号化処理部７０２は、アプリケーション７０１だけでなく、携帯端末１０３の暗号化通信処理部７０４にも利用される。

【００４３】携帯端末１０３では、通信基本処理部７０５の上に、暗号化通信処理部７０４が構成され、さらにその上に、携帯端末アプリケーション７０３が構成される。通信基本処理部７０５は、携帯端末１０３の通信の基本的な処理、例えば、通信路符号化、通信速度の変更、データの送受信などの処理を行う。暗号化通信処理部７０４は、送受信するデータをサーバ１８０との間で取り決めた暗号化方式を用いて暗号処理する。暗号化通信に必要なデータの準備や、暗号計算などの処理は、記録装置１２０の暗号化計算部７０２を利用して行われる。携帯端末アプリケーション７０３は、メニュー表示、電子メール機能など、利用者が携帯端末１０３で利用するさまざまなアプリケーションである。サーバ１８０では、ソフトウェアは、基本通信処理部７０６、暗号化通信処理部７０７及びサーバアプリケーション７０８から構成される。基本通信処理部７０６及び暗号化通信処理部７０７は、携帯端末１０３の基本通信処理部７０４及び暗号化通信処理部７０５と同様の動作をする。ただし、暗号化通信処理部７０７は、暗号化に関する処理を行うときに、記録装置１２０を利用しなくてもよい。サーバアプリケーション７０８は、携帯端末１０３に配信するコンテンツ４０２の管理、利用者の管理など、一般的にサーバとして機能するために必要なアプリケーションである。

【００４４】記録装置１２０が、携帯端末１０３を介してサーバ１８０からコンテンツ４０２を取得する場合について説明する。図9に示すように、携帯端末１０３及びサーバ１８０の暗号化通信処理部７０４、７０７が、基本通信処理部７０５、７０６を介して暗号化通信経路８０１を構成する（これは、暗号化された内部通信経路１０９に相当する）。暗号化通信処理部７０４は、記録装置１２０内の暗号化計算部７０２を利用して暗号化に関する計算を行うと共に、利用者に関する情報をサーバ１８０へ送信し、暗号化通信経路８０１で暗号化及び復号化に利用する一時的な鍵情報などを記録する。

【００４５】暗号化通信経路７０１が構成されると、図１０に示すように、記録装置１２０、携帯端末１０３及びサーバ１８０の各アプリケーションが起動する。記録装置１２０のアプリケーション７０１が、携帯端末１０３と暗号化通信経路７０１を介して、サーバアプリケーション７０８から取得したいコンテンツ４０２に対応するライセンス４０１を取得し、記憶装置１２０のタンパレジスタントモジュール121へ保存する。

【００４６】ライセンス４０１の取得が終了すると、図１１に示すように、記録装置１２０のアプリケーション７０１が、携帯端末１０３と暗号化通信経路８０１を介して、サーバアプリケーション７０８から暗号化コンテンツ４０１を取得し、携帯端末１０３のフラッシュメモリ１４０へ保存する。尚、コンテンツ４０１がすでに暗号化されているため、この手順では、単にサーバ１８０から受信したデータを記録装置１２０へ保存するだけでよいので、物理アクセスコマンド４０８のみを用いて処理を行う。論理アクセスコマンド４０９を利用してもかまわない。

【００４７】図１２は、図8～図１１における通信の処理手順を示したフロー図である。アプリケーション起動処理が実行される（１１００）。携帯端末１０３は、携帯端末１０３が行う通信に必要な処理をするアプリケーションを記録装置１２０内から選択する(１１０１)。ＣＰＵ１２８は、携帯端末１０３に選択されたフラッシュメモリ１４０に格納されているアプリケーションが暗号化されているかチェックする(１１０３)。暗号化されている場合は、ＣＰＵ１２８は、秘密情報Km１５１を用いてアプリケーションを復号化して、アプリケーションRAM１２７に格納する（１１０４）。暗号化されていない場合は、ＣＰＵ１２８は、そのままフラッシュメモリ１４０より読み出して、アプリケーション RAM１２７に実行可能な状態で格納する。ＣＰＵ１２８は、アプリケーションを実行する（１１０６）。

【００４８】アプリケーションが起動すると、携帯端末１０３及び記憶装置１２０は、暗号化通信経路確立処理５００を実行して、サーバ１８０と通信経路を確立する。

【００４９】記憶装置１２０とサーバ１８０との間で送受信処理１１２０が実行される。このとき、暗号化通信経路確立処理５００の暗号化内部通信経路確立処理５２０で使用した秘密情報Ki１５５を利用してサーバ１８０と記録装置１２０が互いのデータを暗号化し、携帯端末１０３を中継して送受信を行う（１１０７～１１１８）。携帯端末１０３は、記憶装置１２０が送受信しているデータを見ることはできない。携帯端末１０３は、記録装置１２０の送信終了を示すデータだけを識別することができるため、該当するデータが記憶装置１２０から送信されてくると、送受信処理１１２０を終了する。

【００５０】携帯端末１０３は、送受信処理１１２０を終了するため、終了処理１１３０を実行する。具体的には、携帯端末１０３は、処理終了通知を記録装置１０３とサーバ１８０へ送信する（１１３２、１１３５）ことでサーバ１８０に通信経路を破棄させ（１１３３）、記録装置１２０にアプリケーションを終了させる（１１３６）。

【００５１】図１３は、サーバ１８０から記録装置１２０へ、携帯端末１０３を経由してライセンス４０１をダウンロードする場合の具体的コマンドのやり取りを示した図である。説明は図１２と対応付けて行う。

【００５２】アプリケーション起動処理１１００では、以下のコマンドがやり取りされる。OPEN_CHANNEL １２０１は、携帯端末１０３から記録装置１２０へ、両者間で仮想の通信経路を構成するために発行されるコマンドである。記録装置１２０は、仮想通信経路の番号を返す。以後の通信は、仮想通信経路番号を利用して行われる。

【００５３】OPEN_FILE １２０２は、携帯端末１０３が記録装置１２０内のライセンス４０１を保存するファイルを指定するコマンドである。記録装置１２０は、指定されたファイルの割り当て番号を返す。以後の処理はこのファイル割り当て番号を利用して行われる。ＶＥＲＩＦＹ　１２０３は、携帯端末１０３が記録装置１２０内のアプリケーションを起動するための認証コードを発行するコマンドである。記録装置１２０が認証コードが正規のものであると認証すると、記録装置１２０内部のアプリケーションが起動され、OPEN_FILE １２０２で指定したファイルがアクセスできるようになる。

【００５４】公衆回線における暗号化された通信経路確立処理５１０が行われる。暗号化内部通信経路確立処理５２０では、以下のコマンドがやり取りされる。SEND_CERT １２０５は、携帯端末１０３が、記録装置１２０へ正当な記録装置１２０あることを証明する証明書の送信を要求するコマンドである。記録装置１２０は、証明書を携帯端末１０３へ送信する。

【００５５】OPEN １２０６は、携帯端末１０３が、記録装置１２０から読み出した証明書とContentIDをサーバ１８０へ送信するコマンドである。証明書をサーバ１８０が認証すると、サーバ１８０は、セッション鍵Ks1を生成して携帯端末１０３へ送信する。SET_SESSION_KEY １２０７は、携帯端末１０３が、サーバ１８０から受信したセッション鍵Ks1を記録装置１２０へ送信するコマンドである。尚　SEND_CERT１２０５、OPEN １２０６及びSET_SESSION_KEY １２０７のコマンドは、図７のコンテンツ要求６０１とセッション鍵Ks1送信６０２に対応する。

【００５６】送受信処理１１２０では、以下のコマンドがやり取りされる。ESTABLISH_WRITE_SESSION　１２０８は、記録装置１２０がセッション鍵Ks2を生成し、それをKs1で暗号化したものを携帯端末１０３へ送信するコマンドである。

【００５７】ESTABLISH_WRITE_SESSION １２０９は、携帯端末１０３が、記録装置１２０から受信したKs1で暗号化されたKs2をサーバ１８０へ送信するコマンドである。暗号化されたKs2を受信したサーバ１８０は、Ｋｓ１で暗号化Ks2を復号し、Ｋｓ２でライセンス４０１を暗号化して、携帯端末１０３へ暗号化されたライセンス４０１を送信する。

【００５８】SET_LICENSE１２１０は、携帯端末１０３が、ライセンス４０１を記録装置１２０へ送信するコマンドである。

【００５９】WRITE_LICENSE1２１１は、携帯端末１０３が、記録装置１２０に、ライセンス４０１をKs2で復号化し、タンパレジスタントモジュール１２１のNVメモリ１２５へライセンス格納領域を作成しそこに格納させるために発行するコマンドである。尚、ESTABLISH_WRITE_SESSION　１２０８、１２０９、SET_LICENSE１２１０及びWRITE_ LICENSE　１２１１は、図７のKs1でセッション鍵Ｋｓ２送信６０３及びライセンス送信６０４に対応する。

【００６０】終了処理１１３０では、以下のコマンドがやり取りされる。CLOSE １２１２は、携帯端末１０３が、サーバ１８０へライセンス取得処理が終了したことを知らせるコマンドである。CLOSE １２１２をサーバ１８０が受信すると、サーバ１８０は、携帯端末１０３とサーバ１８０の間の暗号化通信経路８０１を破棄する。CLOSE_FILE１２１３は、携帯端末１０３が、記録装置１２０のファイルを閉じるために発行するコマンドである。CLOSE__CHANNEL１２１４は、携帯端末１０３が記録装置１２０との間で利用していた仮想通信経路を閉じて処理を終了するために発行するコマンドである。図１４は、サーバ１８０から記録装置１２０へ携帯端末１０３を経由してコンテンツ４０２がダウンロードされる場合のコマンドのやり取りを示す図である。説明は図１１と対応付けて行う。

【００６１】公衆回線１０８における暗号化された通信経路確立処理５１０が行われる。送受信処理１１２０では、以下のコマンドがやり取りされる。OPEN １３０１は、携帯端末１０３が、取得したいContentIDをサーバ１８０へ送信するコマンドである。ContentIDをサーバ１８０が受信すると、サーバ１８０は、暗号コンテンツ４０２を携帯端末１０３へ送信する。SET_BLOCKS_TRANSFERRED １３０２は、携帯端末１０３が、サーバ１８０から受信した暗号化コンテンツ４０２のサイズを記録装置１２０へ送信するためのコマンドである。WRITE_BLOCK １３０３は、携帯端末１０３が、サーバ１８０から受信した暗号化コンテンツ４０２を記録装置１２０内のフラッシュメモリ１４０上の任意のアドレスへ転送するためのコマンドである。アドレスの指定方法としては、フラ

ッシュメモリ１４０上にファイルシステムを設け、ContentIDを元に暗号化コンテンツ４０２に対応するファイルが作成され、ファイルシステムが定めたアドレスを指定する方法などが考えられる。暗号化コンテンツ４０２の容量が大きい場合は、SET_BLOCKS_TRANSFERRED １３０２及びWRITE_BLOCK １３０３が複数回発行される場合もある。

【００６２】CLOSE １３０４は、携帯端末１０３が、サーバ１８０へライセンス取得処理が終了したことを知らせるコマンドである。CLOSE １３０４をサーバ１８０が受信すると、サーバ１８０は、携帯端末１０３とサーバ１８０の間の暗号化通信経路を破棄する。尚、図１４の手順は、図７のコンテンツ送信６０５に対応する。

【００６３】図１５は、記録装置１２０内の暗号化コンテンツ４０２を携帯端末１０３内のデコーダ回路２０６が再生する場合の概念図である。デコーダ回路２０６は、携帯端末１０３以外の機器に搭載されて使用されることも可能である。記録装置１２０も、携帯端末１０３以外の機器と接続されることも可能である。具体例としては、MP3プレーヤ、ステレオ、ディジタル映像再生機などが考えられる。デコーダ回路２０６は、記録装置１２０のタンパレジスタントモジュール１２１から、再生したい暗号化コンテンツ４０２のライセンス４０１を取り出す。デコーダ回路２０６は、フラッシュメモリ１４０から暗号化コンテンツ４０２を取り出し、暗号化コンテンツ４０２をライセンス４０１で復号化してから再生する。ライセンス送信１４０２は、階層化コマンド４０５を用いて行われる。コンテンツ送信１４０３は、物理アクセスコマンド４０８を用いて行われる。尚、それぞれの送信時のコマンドの構成に付いてはこの限りではない。

【００６４】図１６は、図１５における通信の詳細を示したフロー図である。アプリケーション起動処理（１１００）から、アプリケーションを実行する（１１０６）までの処理は、図１１で説明したフローと同一であるので、説明を省略する。

【００６５】アプリケーションが起動すると、暗号化内部通信路確立処理５２０が実行され、デコーダ回路２０６と記録装置１２０との通信経路が確立される。この場合、デコーダ回路２０６専用の秘密情報Ki１５７を用いて通信経路が確立される。

【００６６】送受信処理１５００が実行され、実際に記録装置１２０とデコーダ回路２０６の間でデータの送受信が行われる。このとき、暗号化内部通信経路確立処理５２０で使用した秘密情報Ki１５７を利用してデコーダ回路２０６と記録装置１２０が互いのデータを暗号化し送受信を行う（１５０１～１５０８）。送受信処理１５００の最中は、携帯端末１０３の制御は、デコーダ回路２０６によって行われている。送受信が終了すると、デコーダ回路２０６は、携帯端末のＣＰＵ２０１に終了割り込みを知らせるコマンドを送付する。終了割り込みのコマンドを受けたＣＰＵ２０１は、終了処理１５１０を開始する。具体的には、携帯端末１０３のＣＰＵ２０１は、処理終了通知を記録装置１２０に送信して（１５１２）、アプリケーションを終了させる（１５１３）。

【００６７】図１７は、デコーダ回路２０６が、ライセンス４０１を取得する際の記録装置１２０との間での手順のコマンドを示したものである。説明は図１６と対応付けて行う。尚、図１７においては表記法規定２１０１のデータの所在で秘密情報Ki１５５と記載されているところは、すべて秘密情報Kiに置き換わる。また、Ks5は記録装置１２０の暗号処理回路１２６が乱数などを使用して生成し、Ks6はデコーダ回路２０６の暗号処理回路３０４が乱数などを使用して生成する。

【００６８】アプリケーション起動処理１１００では、以下のコマンドがやり取りされる。OPEN_CHANNEL １６００は、デコーダ回路２０６が、記憶装置１２０との間で仮想の通信経路を確立するために、携帯端末１０３の記録装置インタフェース２０７を介して記録装置１２０へ発行するコマンドである。OPEN_CHANNEL １６００コマンドを受け取った記録装置１２０は、仮想通信経路の番号を返す。以後の通信は、この仮想通信経路番号を利用して行われる。

【００６９】OPEN_FILE １６０１は、デコーダ回路２０６が、記録装置１２０内のライセンス４０１が保存されているファイルを指定するためのコマンドである。OPEN_FILE １６０１コマンドを受け取った記録装置１２０は、指定されたファイルの割り当て番号を返す。以後の処理はファイル割り当て番号を利用して行われる。

【００７０】ＶＥＲＩＦＹ　１６０２は、デコーダ回路２０６が、記録装置１２０内のアプリケーションを起動するための認証コードを発行するコマンドである。記録装置１２０が認証コードが正規のものであると認証すると、記録装置１２０内部のアプリケーションが起動され、OPEN_FILE １６０１で指定したファイルがアクセスできるようになる。

【００７１】秘密情報Ki１５７が使用される暗号化内部通信経路確立処理５２０では、以下のコマンドがやり取りされる。

【００７２】VERIFY_CERT １６０４は、デコーダ回路２０６が、証明書を記録装置１２０へ送信するコマンドである。VERIFY_CERT １６０４コマンドを受信した記録装置１２０は、証明書を認証する。

【００７３】ＳＥＮＤ＿ＳＥＳＳＩＯＮ＿ＫＥＹ１６０５は、記録装置１２０が、デコーダ回路２０６へ暗号処理回路１２６で生成したセッション鍵Ks5を送信するコマンドである。ESTABLISH_PLAY_SESSION１６０６は、Ks5を受け取ったデコーダ回路２０６が、暗号処理回路３０４で生成したセッション鍵Ks6を生成し、Ks6をKs5で暗号化して記録装置１２０へ送信するコマンドである。

【００７４】送受信処理１５００では、以下のコマンドがやり取りされる。ＲＥＡＤ＿ＬＩＣＥＮＳＥ１６０７は、デコーダ回路２０６が、記録装置１２０へ読み出すライセンス４０１の準備を指示するコマンドである。SEND_PLAY_LICENSE１６０８は、デコーダ回路２０６が、記録装置１２０からライセンス４０１を読み出すコマンドである。

【００７５】終了処理１５１０では、以下のコマンドがやり取りされる。CLOSE_FILE１６０９は、デコーダ回路２０６が、記録装置１２０のファイルを閉じるために発行するコマンドである。CLOSE_CHANNEL１６１０は、携帯端末１０３が、記録装置１２０との間で利用していた仮想通信経路を閉じて処理を終了するために発行するコマンドである。

【００７６】図１８は、ライセンス４０１の取得を終了したデコーダ回路２０６が、記録装置１２０から再生を行う暗号化コンテンツ４０２を読み出す処理を示した図である。尚、この手順に付いては、コンテンツ４０２がすでに暗号化されているため、単に記録装置１２０からデコーダ回路２０６へデータを読み出すだけでよいので、物理アクセスコマンド４０８のみを用いて処理を行う。論理アクセスコマンド４０９を利用してもかまわない。

【００７７】図１８の処理では、以下のコマンドがやり取りされる。SET_BLOCKＬＥＮ　１７０４は、デコーダ回路２０６が、読み出す暗号化コンテンツ４０２のサイズを記録装置１２０へ送信するコマンドである。SENT_BLOCKS_TRANSFERRED　１７０５は、デコーダ回路２０６が、記録装置１２０内の暗号化コンテンツ４０２を一度に読み出す量を指定するコマンドである。ＲＥＡＤ_BLOCK　１７０６は、デコーダ回路２０６が、再生する暗号化コンテンツ４０２のアドレスを記録装置１２０へ指定して暗号化コンテンツ４０２を読み出し、再生を行うために発行するコマンドである。

【００７８】このような構成とすることによって、安全にかつ大容量のデータを保存することが出来る。

【００７９】

【発明の効果】本発明では、タンパレジスタントモジュール及び大容量フラッシュメモリを搭載する記憶装置で秘匿性の高いデータを暗号化して大容量フラッシュメモリへ保存するので、データの秘匿性は維持したまま、大容量の秘匿性の高いデータを保持することが可能な安価な記録装置を構成することが出来る。また、記録装置内部で暗号処理を行い、外部機器が暗号鍵や暗号化、復号化を行う必要がないため、外部機器の負担が軽くなる。

【００８０】また、本発明では、タンパレジスタントモジュールにＣＰＵを搭載し、これが外部より送信されてきたデータの秘匿性を様々な条件に応じて判定し、秘匿性の高い情報は、タンパレジスタントモジュール内の不揮発性メモリへ保存し、秘匿性の低い情報は外部のフラッシュメモリへ保存するようにするので、すべてのデータを暗号化する場合に比べてデータ処理が高速で、しかもタンパレジスタントモジュール内の記録領域を有効利用することができる。

【００８１】さらに、本発明では、タンパレジスタントモジュール内で実行するアプリケーションを暗号化して外部フラッシュメモリへ保存し、必要な場合はそれらをフラッシュメモリから読み出し内部のRAMへ展開して実行できるようにすることで、様々なアプリケーションを記録装置に一度に搭載することが可能で、しかも規模の大きなアプリケーションを記録装置内で実行できる。

【図面の簡単な説明】

【図１】本発明を適用した記憶装置の実施形態を示す構成図である。

【図２】本発明を適用した記録装置を利用するシステムの構成を示す図である。

【図３】本発明を適用した記録装置が接続される携帯端末の構成図である。

【図４】携帯端末に搭載されたデコーダ回路の構成図である。

【図５】記録装置と携帯端末そしてサーバ間でのコマンド体系を示す図である。

【図６】暗号化通信経路確立処理のフロー図である。

【図７】携帯端末に接続された記録装置がサーバからコンテンツとライセンスを取得する処理手順を示したフロー図である。

【図８】本発明が適用された各機器のソフトウェアの構成を示す図である。

【図９】本発明における暗号化通信経路の確立を示す図である。

【図１０】本発明におけるライセンスの移動を示す図である。

【図１１】本発明におけるコンテンツの移動を示す図である。

【図１２】本発明におけるダウンロード時の処理手順を示すフロー図である。

【図１３】本発明におけるライセンス取得時のコマンドのやり取りを示すフロー図である。

【図１４】本発明におけるコンテンツ取得時のコマンドのやり取りを示すフロー図である。

【図１５】本発明のコンテンツ再生時の機器の構成を示す図である。

【図１６】本発明における再生時の処理を示したフロー図である。

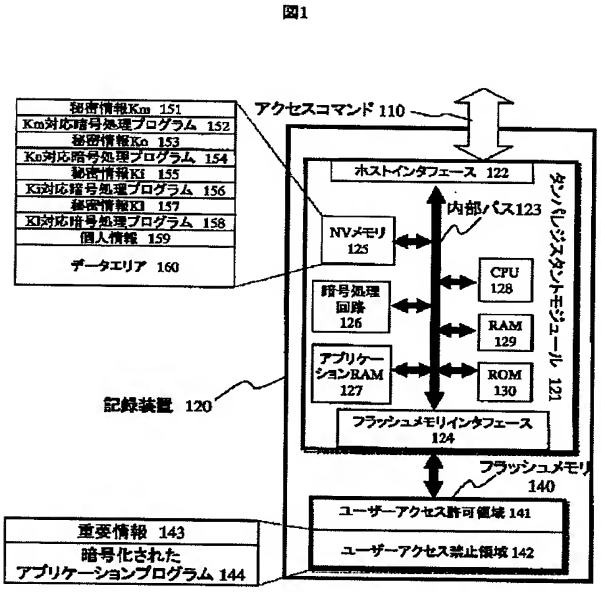
【図１７】デコーダ回路のライセンス取得のコマンドのやり取りを示したフロー図である。

【図１８】デコーダ回路のコンテンツ取得のコマンドのやり取りを示したフロー図である。

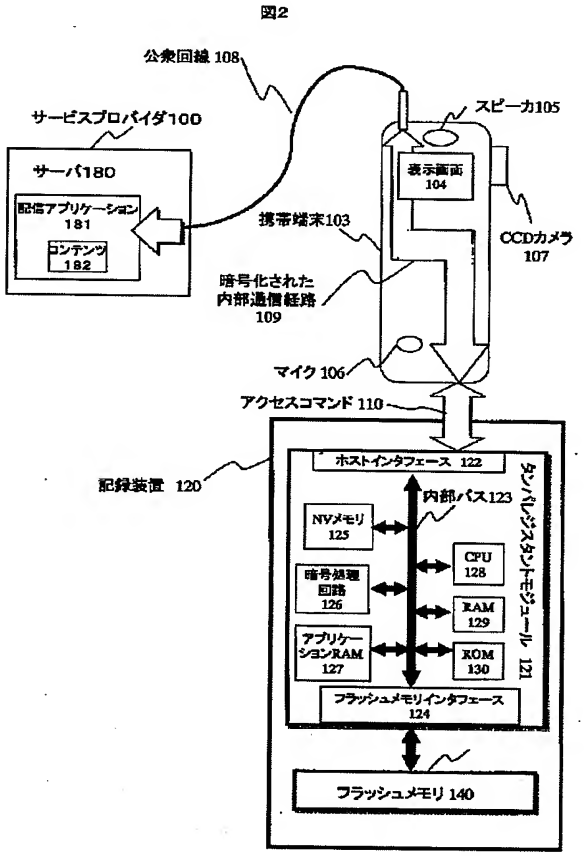
【図１９】本発明におけるアクセスコマンドの構成を示す図である。

【図２０】記録装置のコマンド解析の流れを示したフロー図である。
【図２１】記録装置のデータ選別処理の手順を示したフロー図である。
【図２２】本発明で使用される表記法規定を示す図である。
【符号の説明】
１００…サービスプロバイダ、１０１…配信アプリケーション、１０３…携帯端末、１０８…公衆回線、１０９…暗号化内部通信経路、１１０…アクセスコマンド、１２０…記録装置、１２１…タンパレジスタントモジュール、１２５…NVメモリ、１４０…フラッシュメモリ、１４１…ユーザーアクセス許可領域、１４２…ユーザーアクセス許可領域、１５１…秘密情報Km、１５２…Km対応暗号処理プログラム、１６０…データエリア、２０６…デコーダ回路、４０１…ライセンス、４０２…暗号化コンテンツ、４０３…ネットワーク、４０４…ライセンス配信、４０５、４０６…階層化コマンド、４０７…コンテンツ配信、４０８、４１０…物理アクセスコマンド、４０９、４１１…論理アクセスコマンド、５００…暗号化通信経路確立処理、６０１…コンテンツ要求、６０４…ライセンス送信、６０５…コンテンツ送信、７０１…アプリケーション、７０２…暗号化計算部、７０３…携帯端末アプリケーション、８０１…暗号化通信経路、９０１…ライセンス配信、１００１…暗号化コンテンツ配信、１１００…アプリケーション起動処理、１１２０…送受信処理、１１３０…終了処理、１８０１…コマンドコード、１８０２…長さ、１８０３…データエリア、１８１１…属性、１８１２…セキュリティレベル。

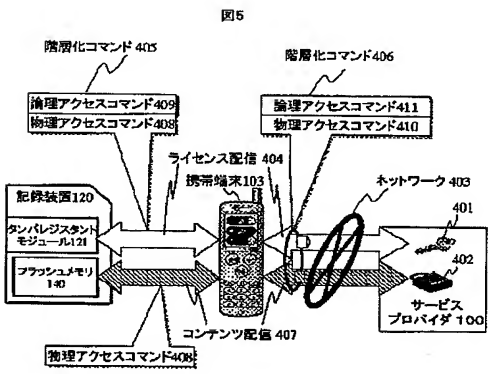
【図１】



【図２】

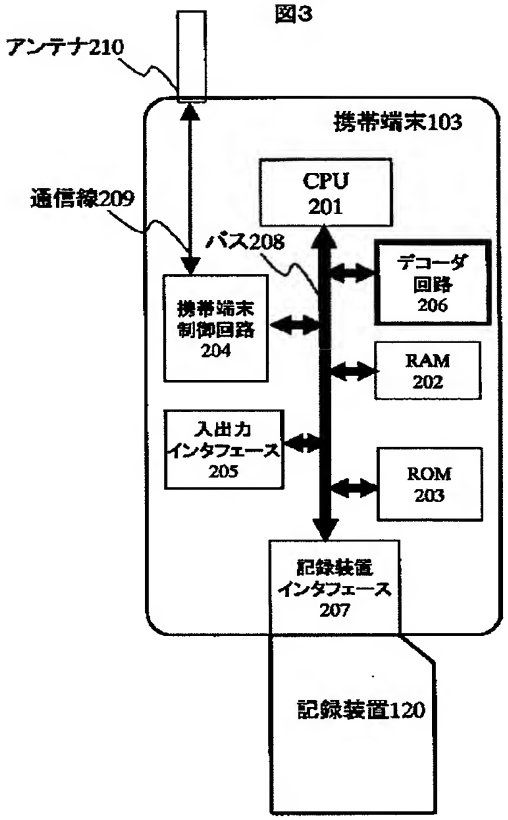


【図５】



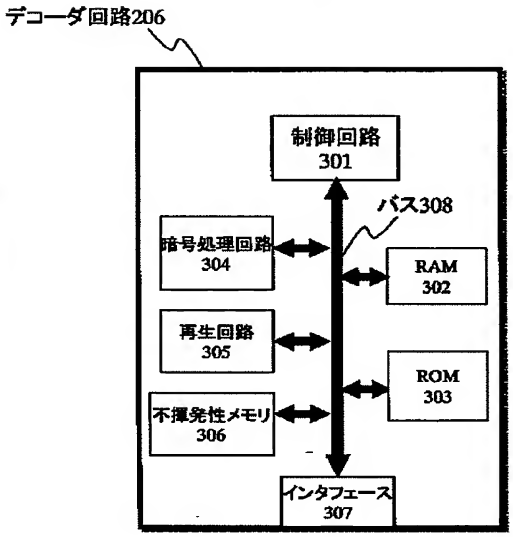
【図３】

図3



【図４】

図4

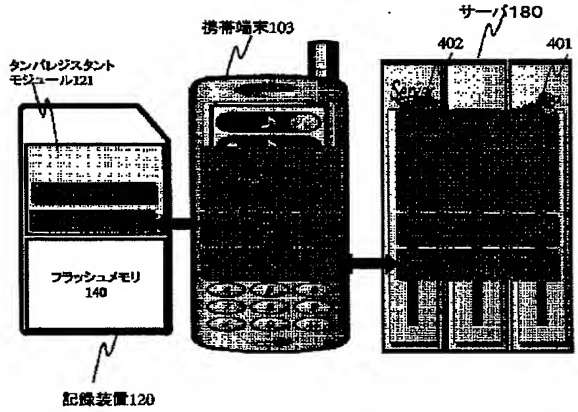


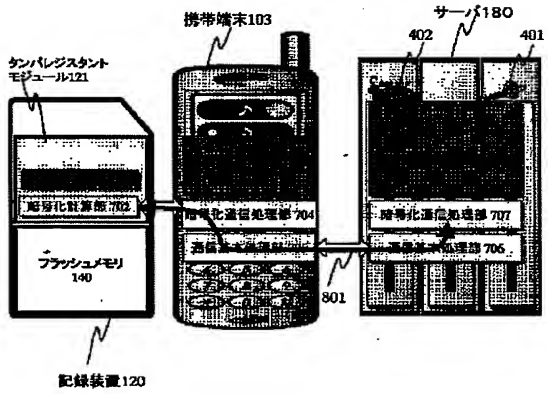
【図９】

図9

【図８】

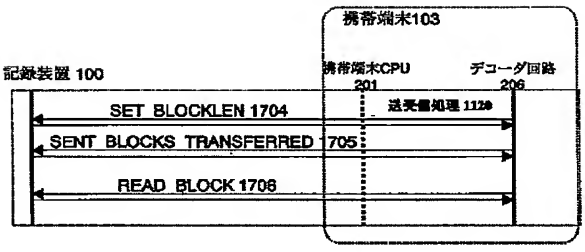
図8





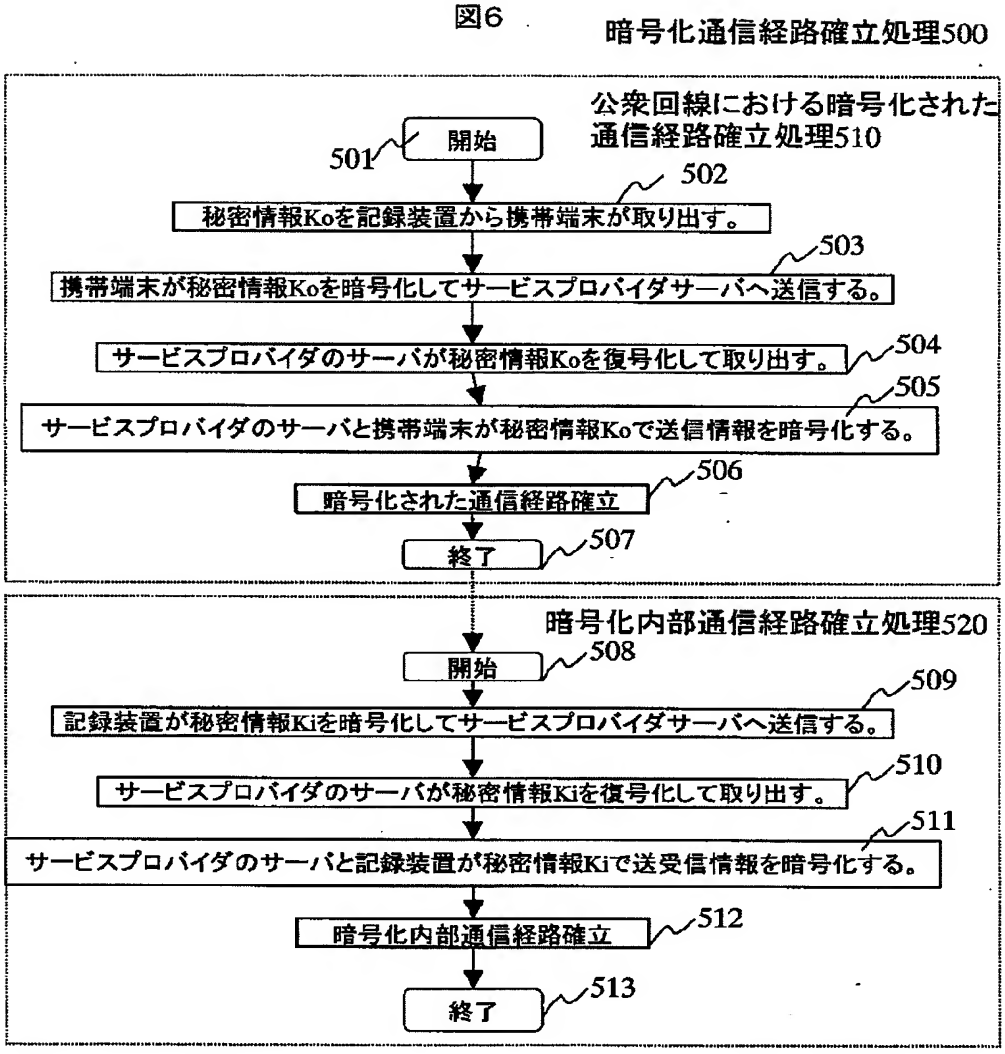
【図１８】

図18



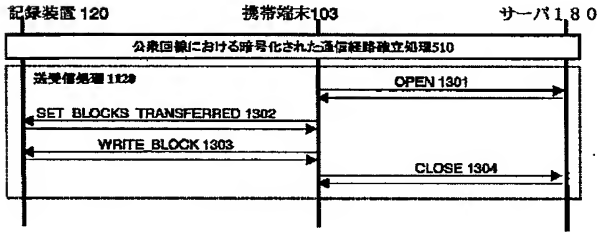
【図６】

図6


暗号化通信経路確立処理500
公衆回線における暗号化された
通信経路確立処理510
開始
501
秘密情報Koを記録装置から携帯端末が取り出す。
502
携帯端末が秘密情報Koを暗号化してサービスプロバイダサーバへ送信する。
503
サービスプロバイダのサーバが秘密情報Koを復号化して取り出す。
504
サービスプロバイダのサーバと携帯端末が秘密情報Koで送信情報を暗号化する。
505
暗号化された通信経路確立
506
終了
507
暗号化内部通信経路確立処理520
開始
508
記録装置が秘密情報Kiを暗号化してサービスプロバイダサーバへ送信する。
509
サービスプロバイダのサーバが秘密情報Kiを復号化して取り出す。
510
サービスプロバイダのサーバと記録装置が秘密情報Kiで送受信情報を暗号化する。
511
暗号化内部通信経路確立
512
終了
513

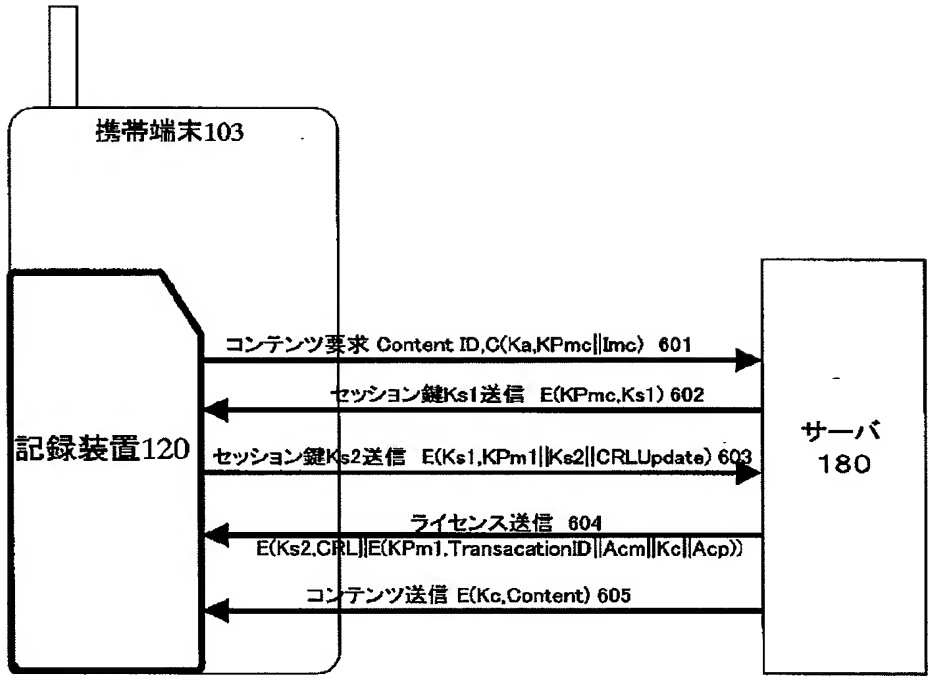
【図１４】

図14


記録装置 120
携帯端末103
サーバ１８０
公衆回線における暗号化された通信経路確立処理510
送受信処理 1129
OPEN 1301
SET_BLOCKS_TRANSFERRED 1302
WRITE_BLOCK 1303
CLOSE 1304

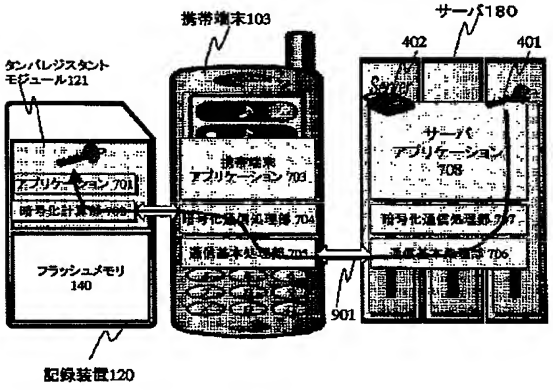
【図7】

図7



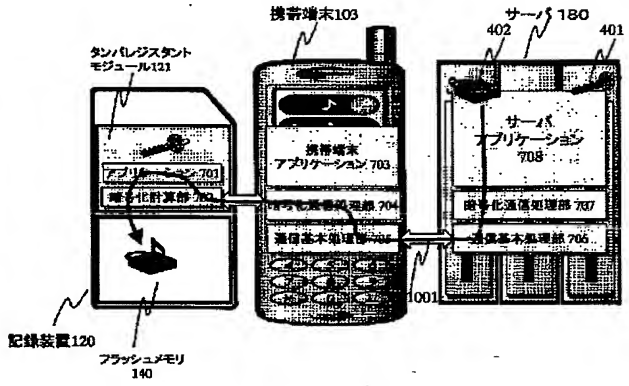
【図10】

図10



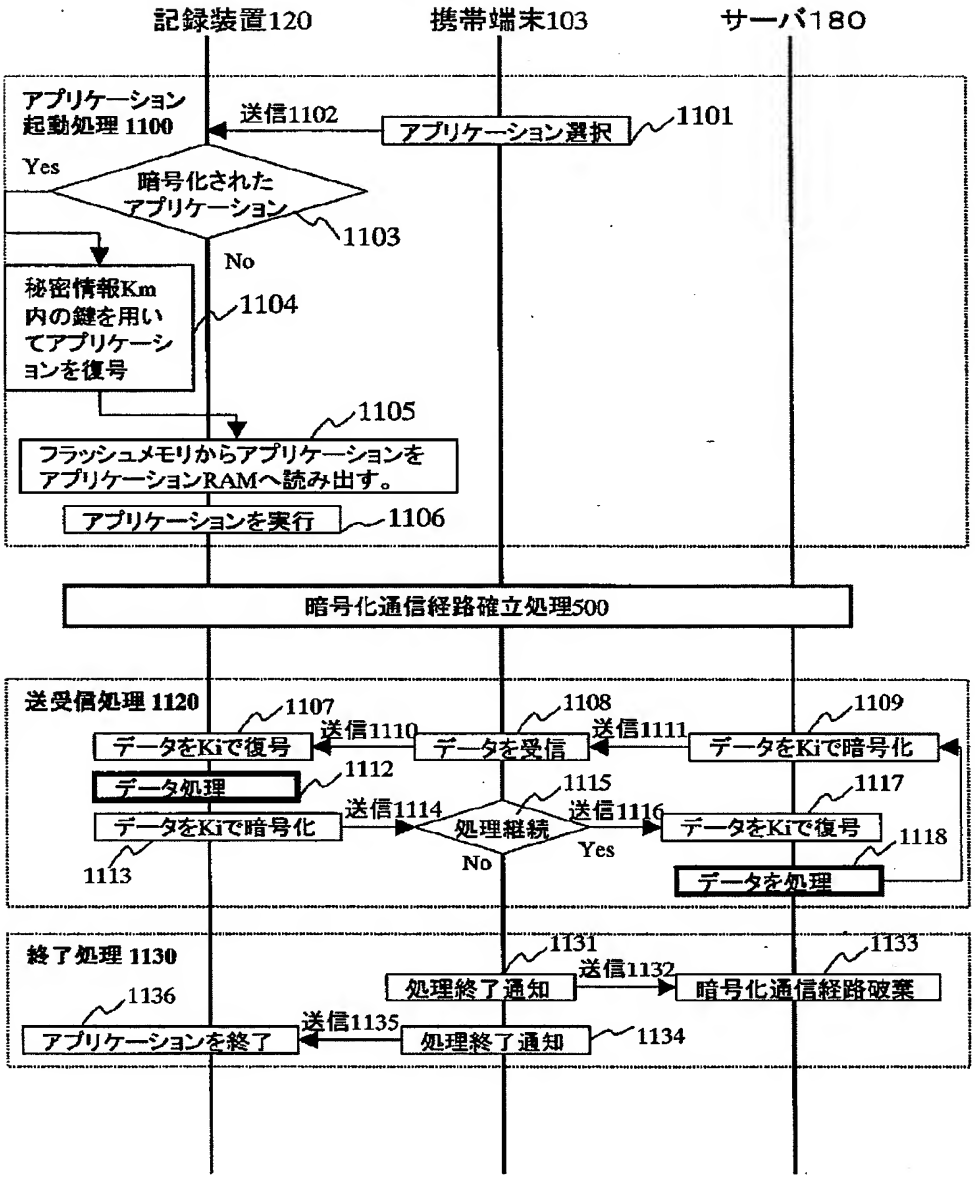
【図11】

図11



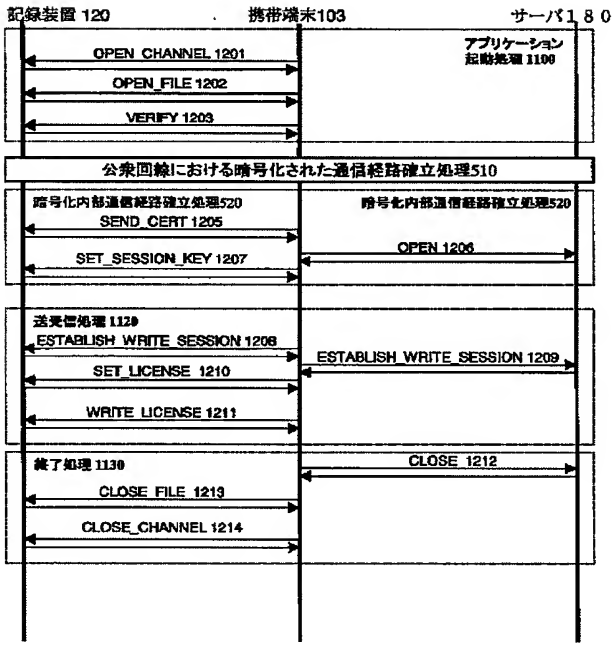
【図１２】

図12


記録装置120
携帯端末103
サーバ180
アプリケーション起動処理 1100
送信1102
アプリケーション選択
1101
Yes
暗号化されたアプリケーション
1103
No
秘密情報Km内の鍵を用いてアプリケーションを復号
1104
1105
フラッシュメモリからアプリケーションをアプリケーションRAMへ読み出す。
アプリケーションを実行
1106
暗号化通信経路確立処理500
送受信処理 1120
1107
データをKiで復号
送信1110
1108
データを受信
送信1111
1109
データをKiで暗号化
データ処理
1112
1115
1117
送信1114
処理継続
送信1116
データをKiで暗号化
データをKiで復号
1118
1113
No
Yes
データを処理
終了処理 1130
1131
1133
処理終了通知
送信1132
暗号化通信経路破棄
1136
送信1135
アプリケーションを終了
処理終了通知
1134

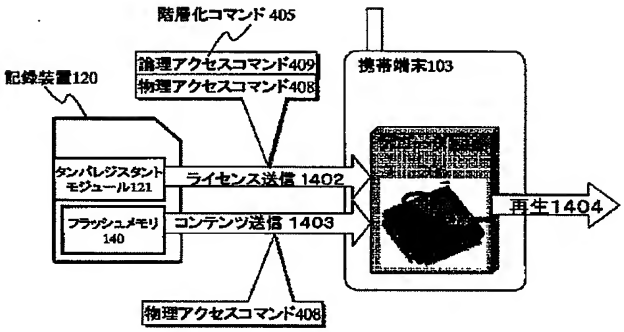
【図13】

図13



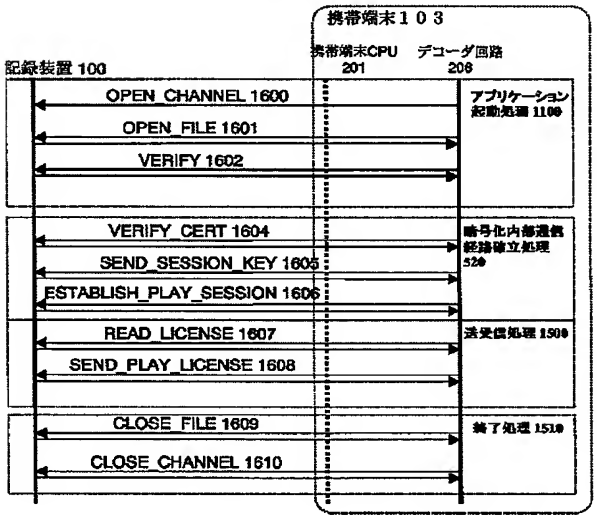
【図15】

図15



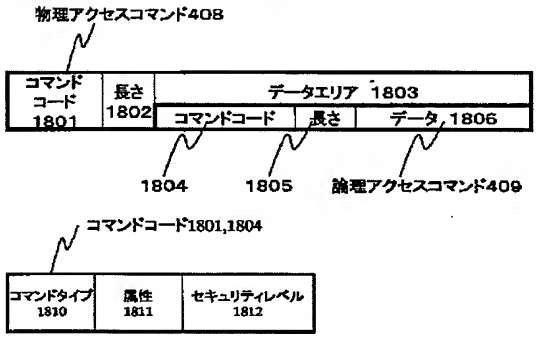
【図17】

図17



【図19】

図19

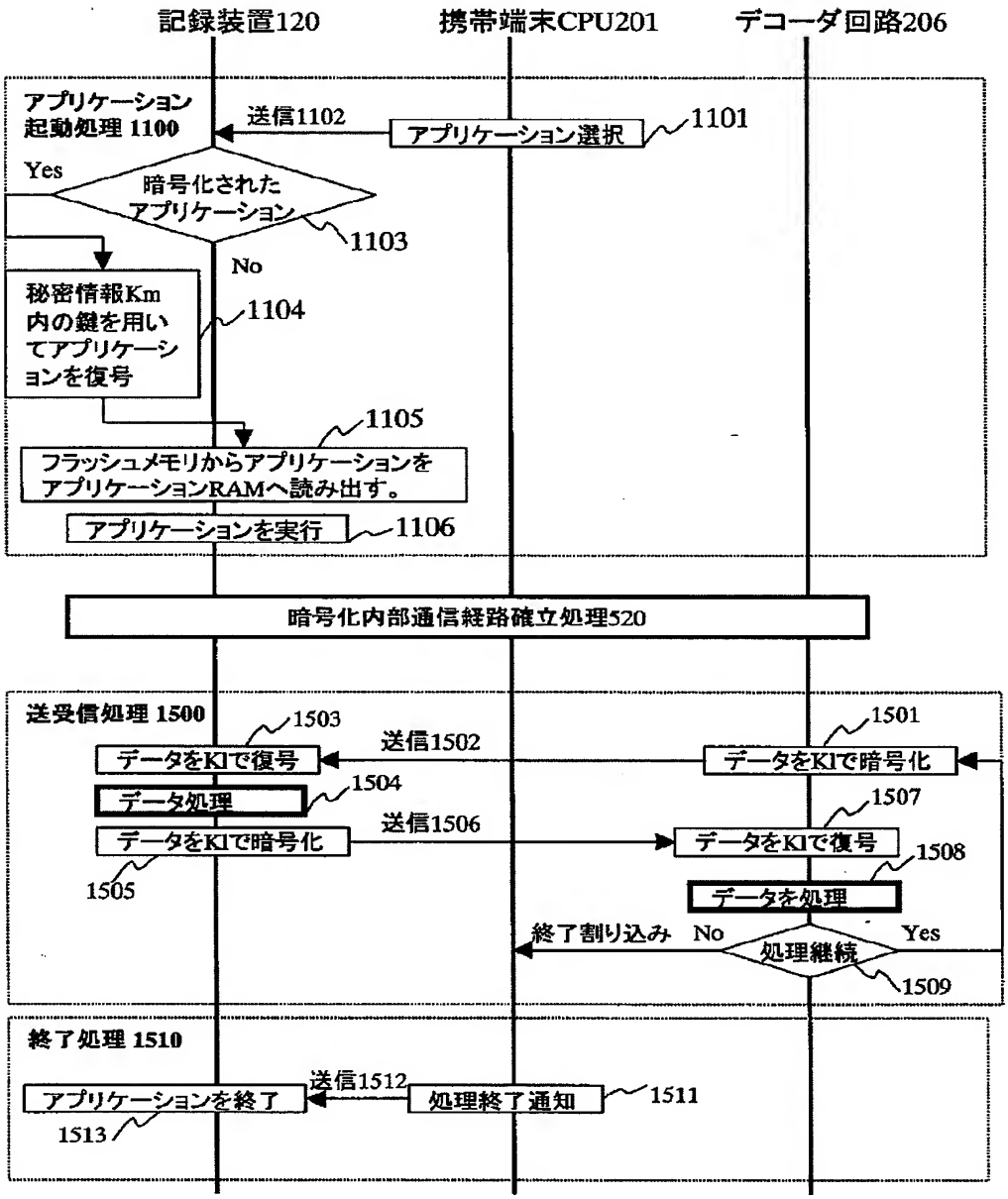


コマンドタイプ1810	属性1811
READ	格納アドレス、データ長
WRITE	格納アドレス、データ長、データ属性
暗号処理	対象秘密情報、処理の種類(暗号化、復号、認証、署名)
アプリケーション実行	対象秘密情報、アプリケーション識別番号
アプリケーションコマンド	実行中のアプリケーションに依存

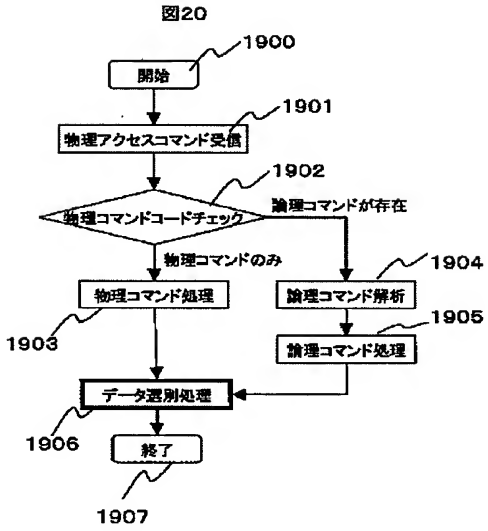
セキュリティレベル1812	説明
1	NVメモリへ格納
2	暗号化して外部メモリへ出力
3	暗号化の必要なし

【図16】

図16


記録装置120
携帯端末CPU201
デコーダ回路206
アプリケーション起動処理 1100
送信1102
アプリケーション選択
1101
Yes
暗号化されたアプリケーション
1103
No
秘密情報Km内の鍵を用いてアプリケーションを復号
1104
1105
フラッシュメモリからアプリケーションをアプリケーションRAMへ読み出す。
アプリケーションを実行
1106
暗号化内部通信経路確立処理520
送受信処理 1500
1503
データをKIで復号
送信1502
1501
データをKIで暗号化
1504
データ処理
1507
送信1506
データをKIで暗号化
データをKIで復号
1508
1505
データを処理
終了割り込み
No
処理継続
Yes
1509
終了処理 1510
送信1512
アプリケーションを終了
処理終了通知
1511
1513

【図20】



【図22】

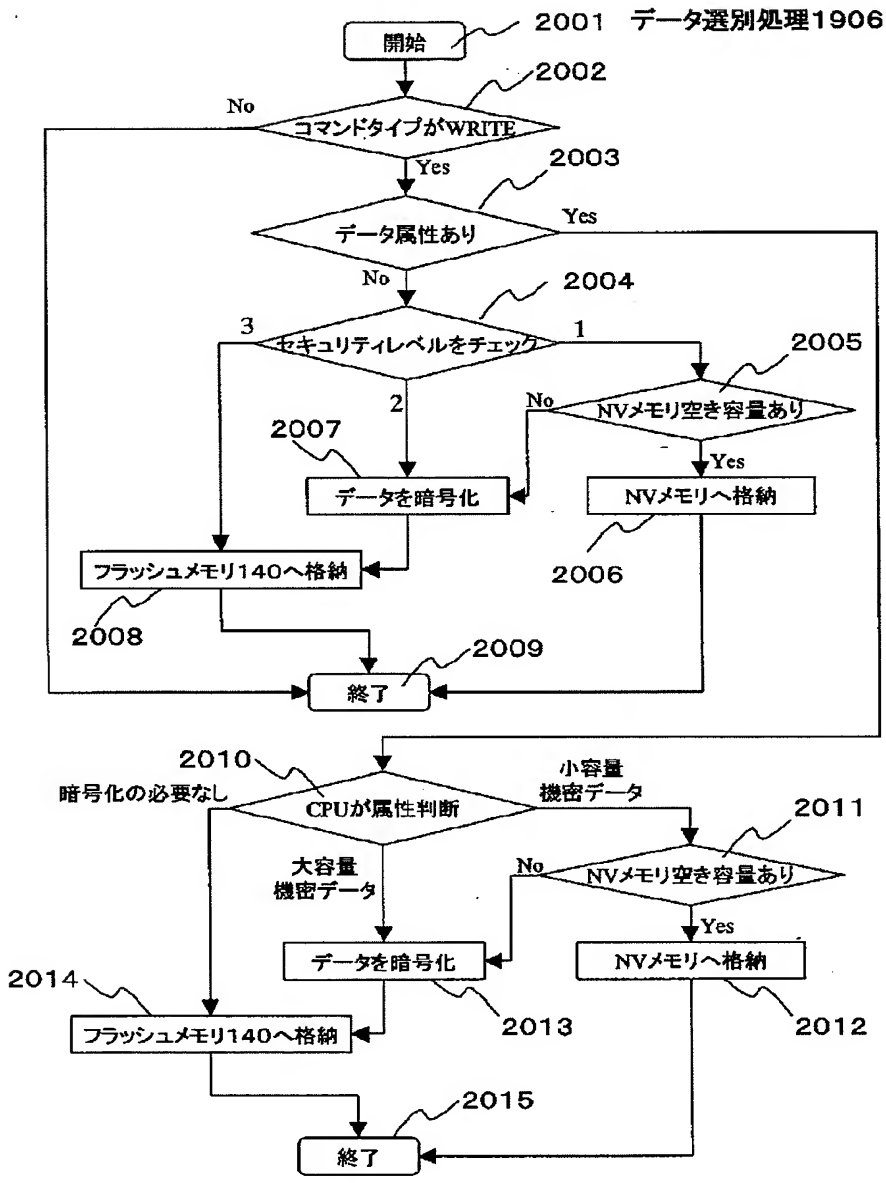
図22

表記法規定2101

名称	表記	データの所在	意味
暗号化	E(K, D)	———	情報Dを鍵Kで暗号化した結果
連結	A‖B	———	情報Aと情報Bを連結した情報
コンテンツID	ContentID	———	コンテンツごとに割り当てられた番号
ルート秘密鍵	Ka	秘密情報Ki	CAで安全に保管されている秘密鍵
メディアクラス秘密鍵	Kmcx	秘密情報Ki	同一メディアクラス(ロット)のチップがその内部に秘密裏に維持する鍵
メディアクラス公開鍵	KPmcx	秘密情報Ki	Kmcxに対応する公開鍵
関連情報	Ixx	秘密情報Ki	xxなどに関連する各種情報
証明書(Certificate)	C(Ka, KPxx‖Ixx)	秘密情報Ki	公開鍵KPxxの証明書 KPxx‖Ixx‖E(Ka, H(KPxx‖Ixx))
トランザクションID	TransactionID	サーバ	トランザクションごとにユニークな識別子値
セッション鍵	Ksx	サーバと秘密情報Ki	通信のセッション毎に，通信エンティティ間で共有する一時的な共通鍵暗号法の鍵
メディア個別秘密鍵	Kmx	秘密情報Ki	各メディアが個別に秘密裏に維持する鍵
メディア個別公開鍵	KPmx	秘密情報Km	Kmxに対応する公開鍵
CRL更新日時	CRLUpdate	秘密情報Ki	CRLを更新した日時
メディアアクセス条件	ACm	ライセンス情報	メディア内部でのデータの扱いについて配信元が強制的に指定したアクセス条件
デコーダアクセス条件	ACp	ライセンス情報	デコーダチップ内部でのデータの扱いについて配信元が強制的に指定したなアクセス条件
コンテンツ鍵	Kc	ライセンス情報	コンテンツ毎に異なるコンテンツ暗号化鍵

【図２１】

図21



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード'(参考)
G06K 19/073		G06F 9/06	660L	5J104
G11C 16/02		G06K 19/00	P	
H04L 9/08		G11C 17/00	601P	
9/10			641	
		H04L 9/00	601A	
			601E	

(72)発明者　角田　元泰
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　石原　晴次
東京都小平町上水本町五丁目20番１号　株式会社日立製作所半導体グループ内
(72)発明者　水島　永雅
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　戸塚　隆
東京都小平町上水本町五丁目20番１号　株式会社日立製作所半導体グループ内

Fターム(参考)　5B017 AA07 BA07 CA15 CA16
5B025 AC00 AE10
5B035 AA01 AA07 AA13 BB09 BB11
BB12 CA02 CA11 CA39
5B065 BA09 PA04 PA14
5B076 BB06 FA20 FB01
5J104 AA01 AA16 EA04 EA18 JA03
NA02 NA35 NA42 PA14